

WHAT IS CLAIMED IS:

1. A method for processing an access-request message for packet service, comprising:

writing a temporary randomly generated authenticator value in an attribute field of an access-request message;

encrypting a user password using the temporary authenticator value;

executing an encryption algorithm using the access-request message having the temporary authenticator value and the encrypted user password to generate a message digest, the access-request message having an authenticator field that is filled with a prescribed value;

generating a final access-request message by replacing the value of the authenticator field with the message digest;

transmitting the final access-request message to an Authentication, Authorization and Accounting (AAA) server; and

verifying the access-request message by the AAA server.

2. The method of claim 1, wherein the prescribed value is a value previously defined between a foreign agent and the AAA server.

3. The method of claim 1, wherein verifying the access-request message comprises:

- temporarily storing the contents of the authenticator field of the access-request message;
- filling the authenticator field with the prescribed value;
- performing an encrypting algorithm to obtain a message digest; and
- verifying the access-request message by comparing the temporarily stored authenticator value to the message digest.

4. The method of claim 3, wherein verifying the access-request message further comprises:

- determining the access-request message to be normal if the authenticator value and the message digest are identical to each other; and
- determining the access-request message to be abnormal if the authenticator value and the message digest are not identical to each other.

5. The method of claim 4, further comprising:

- decoding the access-request message if the access-request message is normal;

and

performing a user authentication by decrypting the encrypted user password written in the attribute field of the decoded access-request message.

6. The method of claim 5, wherein performing the user authentication comprises:

decrypting the encrypted user password written in the attribute field of the access-request message using the temporary authenticator value of the access-request message;

comparing the decrypted user password with the user password stored in a data base;

determining the user authentication to be successful if the decrypted user password and the stored user password are identical to each other; and

determining the user authentication to have failed if the decrypted user password and the stored user password are not identical to each other.

7. The method of claim 4, further comprising discarding the access-request message.

8. The method of claim 1, wherein the randomly generated authenticator value is created differently every time a message is generated.

09934477.022304
T02220.7442660

9. A method for processing an access-request message for a packet service in a communication system, comprising:

writing an authenticator value for authenticating an access-request message in an authenticator field of an access-request message and transmitting an access-request message;

verifying the access-request message by using the authenticator value of the access-request message when the access-request message is received;

decoding the access-request message if the access-request message is successfully verified; and

performing user authentication by decrypting an encrypted user password of the decoded access-request message using a temporary authenticator value of the decoded access-request message and a shared secret key that is known to each of a message transmitter and a message receiver.

10. The method of claim 9, wherein verifying the access-request message comprises:

temporarily storing the authenticator value written in the authenticator field of the received access-request message;

replacing the authenticator value with a prescribed value in the authenticator field, the prescribed value being previously defined between the message transmitter and the message receiver to form a verification access-request message;

performing an encrypting algorithm using the verification access-request message and the shared secret key to form a message digest; and

comparing the message digest with the temporarily stored authenticator value, wherein the access-request message is verified if the message digest and the authenticator value are identical to each other, and wherein the access-request message is abnormal if the message digest and the authenticator value are not identical to each other.

11. The method of claim 9, wherein performing user authentication comprises:

decrypting the encrypted user password written in an attribute field of the decoded access-request message using the temporary authenticator value of the decoded access-request message;

comparing the decrypted user password and a user password stored in a database;

determining that the user authentication is successful if the decrypted user password and the stored user password are identical to each other; and

determining that the user authentication has failed if the decrypted user password and the stored user password are not identical to each other.

12. The method of claim 9, wherein transmitting the access-request message comprises:

encrypting a user password using the temporary authenticator value;

creating the authenticator value for authentication of the access-request message using the temporary authenticator value and a prescribed value previously defined between the message transmitter and the message receiver; and

writing the authenticator value in the authenticator field and generating the access-request message.

13. The method of claim 12, wherein encrypting the user password comprises:

generating an arbitrary value which is differently created each time a message is generated as a temporary authenticator value;

writing the temporary authenticator value in the attribute field of the
access-request message; and

encrypting the user password using the temporary authenticator value and the shared secret key.

14. The method of claim 12, wherein generating the authenticator value comprises:

forming the access-request message by filling attribute fields of the access-request message with the temporary authenticator value and the encrypted user password, and filling the authenticator field with the prescribed value;

executing an encryption algorithm using the generated access-request message and the shared secret key to form a message digest; and

taking the message digest as the authenticator value.

15. The method of claim 12, wherein the temporary authentication value is randomly generated each time a new access-request message is generated, such that the temporary authenticator value is not known beforehand.

16. The method of claim 9, wherein the message transmitter is a Foreign Agent (FA) and wherein the message receiver is an Authentication, Authorization, and Accounting (AAA) server.

17. A method of processing an access-request message, comprising:
receiving an access-request message having a code field, an identifier field, a length field, and authenticator value, and at least one attribute field, the authenticator value being a message digest created by encrypting a temporary access-request message, and the at least one attribute field including an encrypted user password;

processing the authenticator value to determine if the access-request message is a valid access-request message or an abnormal access-request message; and

performing user authentication if it is determined that the access-request message is a valid access-request message and discarding the access-request message if it is determined that the access-request message is abnormal.

18. The method of claim 17, wherein the access-request message is formed by writing a temporary randomly generated authenticator value in a first attribute field of a temporary access-request message, writing a prescribed value into an authenticator field of the temporary access-request message and writing the encrypted password into a second attribute field, encrypting the user password using the temporary authenticator value, executing an encryption algorithm on the temporary access-request message to form a message digest, replacing the temporary authenticator value of the temporary access-request message with the message digest to form the access-request message.

19. The method of claim 17, wherein processing the authenticator value comprises:

temporarily storing the authenticator value written in the authenticator field of the received access-request message;

replacing the authenticator value with a prescribed value in the authenticator field to form a verification access-request message, the prescribed value being previously defined between the message transmitter and the message receiver;

performing an encrypting algorithm using the verification access-request message and a shared secret key to form a message digest; and

comparing the message digest with the temporarily stored authenticator value, wherein the access-request message is verified if the message digest and the authenticator value are identical to each other, and wherein the access-request message is abnormal if the message digest and the authenticator value are not identical to each other.

20. An improved method of processing an access-request message at a message receiving point, the improvement comprising authenticating the access-request message prior to performing user authentication of the access-request message such that abnormal access-request messages are not processed for user authentication.

21. The improvement of claim 20, wherein authenticating the access-request message comprises:

temporarily storing contents of an authenticator field of the access-request message;

filling the authenticator field with a prescribed value known to each of a message origination point and the message receiving point to form a temporary access-request message;

performing an encrypting algorithm on the temporary access-request message to obtain a message digest; and

verifying the access-request message by comparing the temporarily stored authenticator value to the message digest.

22. The improvement of claim 21, wherein verifying the access-request message comprises determining the access-request message to be normal if the authenticator value and the message digest are identical to each other, and determining the access-request message to be abnormal if the authenticator value and the message digest are not identical to each other.

23. The method of claim 22, wherein if the access-request message is determined to be abnormal based on the authentication procedure, the access-request message is discarded, and wherein if the access-request message is determined to be normal, the message is processed for user authentication.

24. An access-request message, comprising:

a code field to indicate that a message is an access-request message;

an identifier field to identify an access-accept message corresponding to the

access-request message;

a length field to identify a length of the access-request message;

authentication information;

a temporary authenticator field; and

an encrypted user password, wherein the authenticator value comprises a 16 byte message digest resulting from performing a prescribed encryption algorithm using a temporary access-request message containing the temporary authenticator and a known authenticator value that is pre-defined between a message origination point and a message destination point.

25. The message of claim 24, wherein the authenticator value is formed by writing a temporary authenticator value in an attribute field of a temporary access-request message, inserting the known authenticator value into an authenticator field of the temporary access-request message, encrypting the user password using the temporary authenticator value, and executing an encryption algorithm on the temporary access-request message to form a byte message digest.

26. The message of claim 25, wherein the access-request message is formed by replacing the value of the temporary authenticator of the temporary access-request message with the 16 byte message digest to form the access-request message.

27. The message of claim 26, wherein the temporary authenticator is randomly generated.

120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000